# Exhibit 1-47

## Conditionally Filed Under Partial Seal

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ALICE SVENSON, individually and on behalf of all others similarly situated,

*Plaintiff*,

v.

GOOGLE, INC., and GOOGLE PAYMENT CORP.,

*Defendants*.

Case No.: 5:13-cv-04080-BLF

CLASS ACTION

**PLAINTIFF'S *CORRECTED* RULE 26(a)(2) EXPERT REPORT OF HENRY FISHKIND, Ph.D IN SUPPORT OF CLASS CERTIFICATION**

## I. Introduction

1.0 Plaintiff Alice Svenson through her counsel retained Fishkind and Associates, Inc. to provide expert economic analysis and litigation support in this matter. Specifically, I was asked among other things to: (a) quantify economic damages (using reliable methodologies and models) based on the plaintiff's theories of liability on a class-wide basis, related to Google's unauthorized disclosure of App Buyers' personal identifying information ("PII") to third-party App Vendors; (b) provide this expert report containing my opinions and the bases and reasons for them, with references to the facts or data considered in forming these opinions, and related exhibits; and (c) testifying at a deposition, hearing, and trial as necessary.

2.0 I conducted the research in this engagement. I drafted this expert report and will offer the testimony. Clerical support was provided by other members of my firm. My resume is attached as Exhibit #1, and my court experience as an expert is provided in Exhibit #2. The materials reviewed, considered, made available, or relied upon in rendering these opinions are listed in Exhibit #3. A list of all publications I have authored in the last 10 years is provided in Exhibit #4.

3.0 Our standard hourly fees apply in this engagement, and our compensation does not depend upon the outcome of any case. Our fees are as follows:

| | |
|---|---|
| Dr. Fishkind: | $450/hour for office work, and $900/hour for testimony at trial, hearing, or deposition. |
| Assistants: | $250/hour for research |

## II. Summary of My Qualifications to Provide Expert Opinion in this Matter

4.0 I am an economist with over 30 years of experience in economic analysis and econometric modeling. I am currently the President of Fishkind & Associates, Inc. ("FA"), an economic and financial consulting firm with offices in Orlando and Port St. Lucie in Florida. My clients include state and municipal governments, the U.S. Department of Justice, Fortune 500 Companies, and major property developers, as well as both plaintiffs and defendants in litigation.

5.0 My resume, included as Exhibit #1, documents my qualifications. I have a Ph.D. in economics from Indiana University with specialties in Urban and Regional economics and in Econometrics. I received my B.A. in economics from Syracuse University.

6.0 For nine years I was Research Economist with the Bureau of Economic and Business Research at the University of Florida, and from time to time I served as its Acting Director and its Associate Director. During the course of my work at the Bureau I conducted numerous surveys. I designed, launched, and administered the Bureau's monthly economic confidence index which involved sample surveys of Floridians. I also designed and executed the Bureau's economic forecasting program.

7.0 I have also served on the Florida Governor's Council of Economic Advisors under two different administrations.[1] In addition, I was a founding board member of two publicly traded companies, Summit Properties (NYSE) and Engle Homes (NASDAQ) until both companies were sold.

8.0 As the President of FA, I am regularly engaged to provide valuations of goods and services as well as tangible and intangible properties. My experience includes valuation of market traded goods and services and non-market traded goods and services. I have designed and conducted numerous surveys to support our clients' business decision making and to be used in court proceedings. Those surveys are similar to the types of surveys I have identified for use in this matter.

9.0 I have extensive experience with, and my engagements have often involved, conducting contingent valuation ("CV") surveys to determine the value of intangible goods such as privacy and PII. Specifically, on six previous occasions I was engaged to provide expert economic analysis, reports, and testimony in privacy-related court cases involving PII. For example, in *Fresco et al. v. Automotive Directions, Inc., et al.*, Case No. 0:03-cv-61063-JEM (S.D. Fla.), I was engaged to determine the value of privacy and PII.

10.0 Furthermore, I have been qualified as an expert witness to provide economic value testimony on more than 50 occasions by both the federal and state courts in Florida and in

[1] Governor Bob Graham 1979 – 1986 and Jeb Bush 1999 – 2007.

federal courts in Tennessee and Washington, D.C. I have also served as a court-appointed expert to provide valuation reports to the U.S. Tax Court. Exhibit #2 lists my court experience over the last five years. I have always qualified as an expert, and have never been rejected as an expert on economic analysis or econometric modeling.

## III. Summary of Expert Opinions

11.0 In this case, the Plaintiff complains that Defendants breached their privacy obligations by sharing the Plaintiff's personal identifying information ("PII") with App Vendors in contravention of the Defendants' stated privacy policies prohibiting such sharing. As a result, the Plaintiff and Class Members (or "Buyers") were damaged.

12.0 The Plaintiff and Buyers incurred two types of economic damages:

12.1 The Buyers did not receive the benefit of the bargain when Defendants wrongfully shared their PII in violation of Defendants' privacy policies. The Buyers paid, in part, to have their PII protected in accordance with their contracts with Defendants. To the extent Defendants disclosed their PII beyond what was provided in their contracts, the Buyers did not receive the full benefit of the bargain they paid for.[2]

12.2 The value of the Buyers' PII was diminished by Defendants' failure to adhere to their own privacy provisions contained in their purchase contract and privacy policies. To the extent Defendants disclosed the Buyers' PII beyond what was permitted under their contracts, it diminished the value of the Buyers' PII and deprived the Buyers of the ability to benefit from their PII themselves.[3]

### A. Benefit-of-the-Bargain Damages

13.0 When the Buyers purchased Apps on Defendants' platforms, they paid not only for the Apps themselves, but also for processing, and the right to have Defendants maintain the privacy of their PII except in certain contractually defined circumstances.[4] To the extent Defendants' disclosures of Buyer PII exceeded those contractual circumstances (an issue beyond

---

2 *See* Dkt. 118 at 8.
3 *Id*. at 8 – 9.
4 *Id*. at 6 – 7.

the scope of this Report), the Defendants denied the Buyers the full measure of goods and services paid for.[5]

14.0 I developed a set of three simple algebraic formulae to quantify the benefit-of-the-bargain damages to the Buyers, based upon a large-scale survey that determined the value of the types of PII wrongly disclosed in this case. As discussed in more detail below, there were five different sets of PII disclosed in this case: (1) name and email; (2) state, city, and zip; (3) email, name, city, state and zip; (4) email, name, street, city, and zip; and (5) email, name, street, city, zip, and phone. Each set has a specific value of the PII to the Buyers. For convenience I will identify them as D1 through D5.

15.0 The Plaintiff purchased an App for $1.77. Other Buyers purchased Apps for other prices. For convenience I will term this PRICE for the price of the App purchased by a Buyer.

16.0 To calculate the benefit-of-the-bargain damage to any Buyer, paying any PRICE for their App, that resulted in the wrongful disclosure of any bundle of PII ranging from D1 through D5; the following three simple algebraic formulae are used:

DAMAGE = PRICE X %DISCOUNT

%PRIVACY DELIVERED = PRIVACY VALUE DELIVERED/PRIVACY VALUE UNDER CONTRACT

%DISCOUNT = 1 − %PRIVACY DELIVERED[6]

17.0 DAMAGE equals the price paid for the App ($1.77 by the named Plaintiff but any value paid by any Buyer can be used) times the discount caused by the disclosure of any specific bundle of PII (D1 through D5).

18.0 The Buyers paid for the App, processing, and privacy protection ("PP"). However, the Buyers did not actually receive the PP they paid for, and some components of the

---

[5] *Id* at 8.

[6] I understand from the Complaint, the Court's order on Defendants' Motion to Dismiss, and the discovery documents I have reviewed that Google only retains 30% of the sales price of each App in exchange for its supposedly private processing service. I do not believe this fact to change the damages analysis, because Plaintiffs were making a single, bundled purchase, and the presence or absence of privacy protections affected their willingness to pay for the entire bundle. That said, should the Court determine that the Buyers' damages can be calculated only by reference to amount paid directly to Defendants, the formulae identified above would still be appropriate, with PRICE potentially redefined to equal the portion of the purchase price retained by Defendants, rather than the actual sales price.

PII were wrongfully disclosed (D1 through D5). Using a large-scale, contingent-valuation survey and econometric techniques, I determined the prices that Buyers were willing to pay for PP and for D1 through D5. The %PRIVACY DELIVERED is readily calculated by dividing the prices that Buyers were willing to pay for the privacy provided to them by the contracts (PP) compared to the privacy that was actually delivered (PP1 through PP5). Since Buyers value their privacy, they are willing to pay more for privacy protection than for various bundles of privacy disclosures (PP1 through PP5 in this case). So the ratio of privacy delivered (PP1 through PP5) to privacy contracted for is always less than one.

19.0 The discount is simply one minus the ratio of the price for the privacy actually delivered compared to the price of the contracted-for privacy.

20.0 Given just two pieces of information, the three formulae quantify the benefit-of-the-bargain damage for any Buyer, paying any price for an App, with any one of the five sets of PII wrongfully disclosed. The two pieces of information that are needed are: (1) the value of the set of PII, and (2) the price the Buyer paid for the App (PRICE). Table 1 provides the calculations for the benefit-of-the-bargain damages for the Plaintiff who bought an App for $1.77 in this case. Damages range from $0.24 to $0.55 depending on the type of PII disclosed.

**Table 1. Summary of Plaintiff's Benefit-of-the-Bargain Damages**

| Privacy Disclosure | % Privacy Delivered | Discount | Price | Damage |
|---|---|---|---|---|
| **Disclosure of Name and Email** | 86% | 14% | $1.77 | **$0.25** |
| **Disclosure of State, City, and Zip** | 86% | 14% | $1.77 | **$0.24** |
| **Disclosure of Email, Name, City, State, and Zip** | 85% | 15% | $1.77 | **$0.26** |
| **Disclosure of Email, Name, Street, City, and Zip** | 83% | 17% | $1.77 | **$0.30** |
| **Disclosure of Email, Name, Street, City, Zip, and Phone** | 69% | 31% | $1.77 | **$0.55** |

### B. Damages from the Diminished Value of PII

21.0 In addition to depriving the Buyers the full benefit of their bargain with Defendants, Defendants' disclosure of Buyers' PII diminished the value of that information.[7] PII

[7] *See* Dkt. 118 at 8 – 9.

has value in the marketplace, and its value can be ascertained by reference to the cost to acquire it for standard marketing purposes. In turn, that value depends upon the type of PII and its linkage to specific market transactions. Data that is captured by recording the search activities and/or locations of individuals coupled with their email addresses is more valuable. When the captured data involves actual purchases of goods and services—as is the case here—it is even more valuable. Finally, the value also depends upon the types of goods and services purchased.

22.0 Private firms routinely offer certain types of PII for sale to businesses primarily for generating sales leads. The price offered reflects the value of the PII. Moreover, a number of firms now offer to assist consumers in managing the sale of their PII by bundling together many consumers to better enable the sale of their PII in the marketplace.[8]

23.0 Table 2 identifies the value of various types of PII as determined by the cost of acquiring the set of PII in bundles of 10,000 from various national vendors of sales lead information. Those PII bundles include a generalized set of PII from several different sources, as well as bundles reflective of PII that were wrongly disclosed in this case (*see* paragraph 14.0). On this basis, the types of PII disclosed by Defendants had values of between $0.080 and $0.170 per person, per bundle.

**Table 2. Diminished Value of PII**

| Type/Category of PII | Value |
|---|---|
| **General/Average** | $0.083 |
| **Name and address** | $0.080 |
| **Name, address, and email** | $0.100 |
| **Name, address, and phone number** | $0.100 |
| **Name, address, and email campaign** | $0.110 |
| **Name, address, email, and phone number** | $0.170 |

*Sources: InfoUSA, LeadsPlease.com; The Guardian, Alesco Data, Redidata, and Accurate Leads, Axciom, NAICS Association, LLC, and Nationwide Marketing Services*

24.0 The estimates presented in Table 2 are very conservative because, although the bundles of PII are similar to those wrongly disclosed in this case, the disclosures in this case not only included generic PII, but specifically linked the PII to an actual purchase of a specific App.

[8] As discussed below, the firms include Datacoup, Handshake, and Meeco.

## IV. Background

25.0 The Plaintiff along with other consumers ("Buyers") purchased mobile device software applications ("Apps") from Defendants' online Google Play store (previously known as Android Market) using the Google Wallet online payment service (or its predecessor, Google Checkout).[9] Buyers had to sign up for a Google Wallet account, because Google Wallet was the exclusive payment processing system for purchasing Apps from Google's Play store.[10] Therefore, to make an App purchase, Buyers had to use Google's Wallet service for payment processing. In exchange for providing processing services with privacy protections, Defendants retained 30% of the App purchase price, and provided the remainder to the App Vendors.[11]

26.0 To use Google Wallet and buy an App, Buyers were required to provide PII about themselves to Google, including name, email, address, and other contact information.[12] Moreover, each time a Buyer purchased an App, the Buyer agreed to the Google Wallet Terms of Service, and with it the Google Wallet Privacy Policy,[13] which "describes [Defendants'] privacy practices that are specific to Google Wallet."

27.0 Those contracts represent that Defendants "will only share a Buyer's personal information with other companies or individuals outside of Google: (i) as permitted under the

---

[9] *See* GOOG-00001093 [redacted].

[10] *See* GOOG-00001453 [redacted]

[11] *See* GOOG-00001444 [redacted]; GOOG-00005709 (Merchant Center Help Center page).

[12] *See* GOOG-00009057 [redacted].

[13] *See* GOOG-00000957 (Google Play Terms of Service stating that "When you buy a Product, you contract for the purchase and use of that item is completed once you click the button indicating that your purchase is complete and you are not able to withdraw from the contract after that point . . . When you buy Products from Google Play you will buy them…in the case of Android apps, from the Provider of the app (an 'App Sale') . . . Each time that you purchase a Product, you enter into a contract based on these Terms with: Google in relation to the use of Google Play and (in the case of a Direct Sale) the purchases of that Product; and also (in the case of Agency Sales and App Sales) with the Provider of the Product you have purchased.").

Google Privacy Policy ('GPP'); (ii) as necessary to process the Buyer's transaction and maintain the Buyer's account; and (iii) to complete the Buyer's registration for a service provided by a third party." The Google Wallet Privacy Notice did not inform users that Google would share personal information with App Vendors.[14]

28.0 Defendants continually assure customers that they protect user privacy.[15] "Users entrust us with their information, their e-mail and name, and we will only give it out to anybody in the case that it's needed to make sure you have a good experience."[16] Google's director of privacy stated that: "I think that users should have opportunities to understand about the information, their personal information and how it is shared."[17]

29.0 However, according to Plaintiff's Complaint and as it appears from the discovery, Defendants disclosed to the App Vendors (entirely third parties) Buyers' PII via the Google Wallet portal—the Buyer's identity to include combinations of name, address, city, zip code, email address, or telephone number.[18] Google's decisions to share Buyer PII appear to be largely intentional.[19] For example, when Defendants rebranded Google Checkout as Google Wallet, Defendants additionally told merchants to download Buyer contact information while it was still available.[20] Likewise, Defendants have admitted that PII was disclosed to App Vendors during

---

[14] *See* GOOG-00000998 (Google Wallet Privacy Notice August 1, 2012); *see also* Lawyer Dep. Tr. at 152:58 [redacted]

[15] *See* GOOG-00006988 – 6991 (Google's Privacy Principles); GOOG-00000110113 (Google Privacy Policy stating "Your privacy matters to Google" and "We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.").

[16] Elbouchikhi Dep. Tr. at 96:4 – 7.

[17] You Dep. Tr. at 52:12 – 13.

[18] *See, e.g.*, GOOG-00001941(name), GOOG-00001948 (email), GOOG-00003715 (email), GOOG-00004129 (street address and phone number), GOOG-00003783 (city, state, zip).

[19] *See* Affaki Dep. Tr. at 38:5 – 12 [redacted]

[20] GOOG-00006841 [redacted]; *see also* GOOG-00005613.

the relevant period.[21] App Buyers could not opt out of the sharing of their information.[22]

30.0 Based on my review of the discovery to date, Defendants disclosed PII to App Vendors, including name, email address, street address, city, state, zip code, and telephone number, in the following combinations:[23]

- Buyer name and email address;
- Buyer state, city, and zip code;
- Buyer name, email address, city, state, and zip code;
- Buyer name, email address, city, state, and zip code;
- Buyer name, email, street address, city, state, zip code, and telephone number.[24]

31.0 Plaintiff's Complaint alleges that Defendants' disclosures of PII to App Vendors breach its contracts with Buyers. I understand that Defendants dispute that their disclosures of Buyer PII were in any way improper. Those issues are outside the scope of my analysis and report. However, and directly relevant to the issues discussed in this report, I also understand that Defendants dispute whether Buyers suffered *any* damages as a result of the disclosure of their PII.

32.0 This report provides a methodology for quantifying the damages suffered by Buyers for disclosures of each of the groups of PII identified above. Specifically, this report describes methods and models for calculating class-wide damages under the benefit-of-the-bargain theory and the diminution-of-value theory as applied to this case, and also describes the empirical work done in order to quantify damages under both theories. This report confirms that damages may be calculated on a class-wide basis, based on accepted and sound methodological principles.

---

[21] *See* Defendants' Supp. Interrog. Resp. No. 1 (Feb. 4, 2016).

[22] *See* GOOG-00001610 [redacted]

[23] *See* Defendants' Supp. Interrog. Resp. No. 1 (Feb. 4, 2016).

[24] *See* GOOG-00001941 (name); GOOG-00001948 (email); GOOG-00003715 (email); GOOG-00004129 (street address and phone number); GOOG-00003783 (city, state, zip).

## V. Quantifying the Benefit-of-the-Bargain Damage

### A. Overview of the Methodology

33.0 In this case, the Plaintiff purchased an App for $1.77 on the Google Play Store.[25] As with other Buyers, that purchase entitled Plaintiff to receive the App, as well as Defendants' processing, services and protection of her PII. Discovery has shown Defendants' disclosure of several categories of Buyer PII to App Vendors, which Plaintiff contends were prohibited by the contracts between Buyers and Defendants. Assuming that to be the case, the Plaintiff and the other Buyers were deprived of the full set of benefits of the bargains between themselves and Defendants.

34.0 As mentioned, I developed three simple algebraic formulae to quantify the benefit-of-the-bargain damages to the App Buyers based upon a large-scale survey that determined the value of the types of PII wrongly disclosed in this case. As noted above, the discovery to date has shown that Defendants made various buyer PII available to App Vendors. These three formulae allow for the robust and methodical class-wide calculation of benefit-of-the-bargain damages, taking into account varying purchase prices of Apps as well as varying disclosures of PII by Defendants.

35.0 Specifically, counsel requested that I assume that there were five different sets of PII disclosed in this case throughout the relevant time period: (1) name and email; (2) state, city, and zip; (3) email, name, city, state, and zip; (4) email, name, street, city, and zip; and (5) email, name, street, city, zip, and phone. Each PII set has a specific value to the Buyers, and for convenience I will call them "D1" through "D5."

36.0 By way of example, the Plaintiff purchased her App for $1.77. Other Buyers purchased Apps for other prices. I will call the price of the App purchased by a Buyer "PRICE."

37.0 To calculate the benefit-of-the-bargain damage to any Buyer, paying any PRICE for their App, that resulted in the wrongful disclosure of any bundle of PII ranging from D1 through D5; the following three simple algebraic formulae can be used.

[25] Dkt. 84, ¶ 88.

DAMAGE = PRICE X %DISCOUNT

%PRIVACY DELIVERED = PRIVACY VALUE DELIVERED/PRIVACY VALUE UNDER CONTRACT

%DISCOUNT = 1 − %PRIVACY DELIVERED

38.0 DAMAGE equals the PRICE paid for the App ($1.77 by the named Plaintiff, but any value paid by any Buyer can be used) multiplied by the DISCOUNT caused by the disclosure of any specific bundle of PII (D1 through D5).

39.0 The Buyers paid for the App, processing, and privacy protection ("PP"). However, the Buyers did not actually receive the PP they paid for, because some components of their PII were wrongfully disclosed (D1 through D5). Using a large-scale, contingent valuation survey and econometric techniques (described below), I determined the prices that Buyers were willing to pay to for PP and for D1 through D5. The "%PRIVACY DELIVERED" is readily calculated by dividing the prices that Buyers were willing to pay for the contracted-for privacy (PP) compared to the privacy that was actually delivered ("PP1" through "PP5"). Since Buyers value their privacy, they are willing to pay more for privacy protection than for various bundles of privacy disclosures (PP1 through PP5 in this case). So the ratio of privacy delivered (PP1 through PP5) to contracted-for privacy is always less than one.

40.0 The DISCOUNT is simply one minus the ratio of the price for the privacy actually delivered compared to the price of the contracted-for privacy.

41.0 As noted above, I quantified the value of the PII to any Buyer using a large scale, contingent-valuation survey methodology ("CV") combined with econometric analysis (described below). The methodology I used to develop the survey information is discussed next.

**B. Methodology to Quantify Benefit-of-the-Bargain Damage**

**i. Introduction to the Methodology**

42.0 As described above, this Report measures the damages resulting from Defendants' failure to provide App Buyers with the privacy protections to which they were entitled as part of their App purchases. While the Buyers' purchases can be viewed as including three components: (i) the Apps themselves, (ii) processing, and (iii) the contracted-for privacy

protections; the sales themselves were made in one bundled form—Buyers paid one price for all three components of the transaction. This portion of my Report seeks to establish the value of PII privacy in those transactions.[26]

43.0 While there is a large public market for Apps, the marketplace for privacy or privacy-related promises is not as obvious. Thus, generally speaking (and as explained below), a contingent valuation ("CV") survey as proposed and conducted here is the established and most reliable method for determining benefit-of-the-bargain damages where privacy obligations are breached. [27]

**ii. Review of the Professional Literature Concerning PII and CV Methodology**

44.0 An established and reliable methodology is necessary to calculate damages resulting from breached privacy obligations on a class-wide basis. Economists have developed CV-survey techniques to estimate the value of typically nontraded goods similar to the privacy protections at issue in this case. CV surveys have become widely used and generally accepted for quantifying the value of nontraded goods.[28] Haab (2002) confirms that CV surveys have now become accepted as accurate as experimental approaches for measuring the prices or values of nontraded goods such as privacy and PII at issue here.[29]

45.0 There is a vast literature concerning the valuation of privacy and techniques for quantifying that value.[30] This is partly because privacy has attracted significant world-wide attention among lawyers, politicians, academics, and members of the business community (see Scott 2016). The result of this broad and deep literature related to privacy and privacy valuations is that concrete and reliable methods and models for calculating damages related to privacy violations such as CV surveys have been developed and tested.

---

[26] *See* Dkt. 118 at 7 ("Svenson alleged that a portion of the $1.77 App purchase price compensated Google for the service of facilitating the App transaction without disclosing her personal information; and that she was denied the benefit of her bargain when Google facilitated the App transaction but disclosed her personal information to the third-party vendor.").

[27] *See id.* at 7 – 8.

[28] Kopp, Raymond et al. (1997), Determining the Value of Non-Marketed Goods, Boston, MA: Kluwer Academic Publishers

[29] Haab, Timothy C., and McConnell, Kenneth E., Valuing Environmental and Natural Resources, 2002.

[30] See Appendix #3 for the materials I have reviewed in this matter.

46.0 As a backdrop to the studies confirming the validity of CV surveys, and in surveying the privacy literature, it is clear that despite alternative definitions, "privacy" relates to hiding personal information. Posner (1981), for instance, studied market inefficiencies resulting from firms concealing product defects or people concealing flaws such as criminal records, ill health, or prior social misconduct from employers. Over the past 35 years and in light of the growth in importance of the internet and on-line retailing, the term "privacy" has evolved so that, for individuals, it now largely relates to securing PII such as name, email address, credit card details, and physical location. Releasing PII in connection with consumer transactions can result in economic harms (Shapiro and Varian 1997). Firms may use personal information collected for advertising or spam, or to price discriminate based on a person's shopping habits. Firms may also transmit customer information to third parties for deceptive marketing, identity fraud, or other nefarious purposes. For these reasons, among others, consumers place a value on protecting their PII.

47.0 Accordingly, important privacy research attempts to measure the monetary value that people place on their own PII. A common hurdle for doing this is the so-called "privacy paradox"—the disconnect between what people say their privacy is worth and how they act when their privacy is at stake. For example, Acquisti and Grossklags (2005), found that 90% of their experimental subjects stated that they had a high concern for their own privacy, yet 90% of these same respondents then risked disclosure of their full name and home address in exchange for a supermarket loyalty card. Other studies have come to similar conclusions or discussed the privacy paradox. *See* Beresford, Kübler, and Preibusch (2012); Speikermann *et al.* (2001); Norberg *et al.* (2007); Cvrcek *et al.* (2009); and Carrascal *et al.* (2013) and others present further results along these lines. Godel *et al.* (2012) and Kokolakis (2015).

48.0 In explaining the privacy paradox, Acquisti *et al.* (2013) attribute it to cognitive biases featured prominently in the behavioral economics literature. As discussed by Acquisti (2004), cognitive biases cause privacy preferences to be undervalued: A subject may not appreciate the long-term harms of lost privacy when given a chance to trade it away for a short-term, immediate-gratification, benefit. Others, such as Cofone (2015), disagree.

49.0 Recent empirical studies have further analyzed the presence of the privacy paradox and found that where privacy protections are communicated clearly, individuals are likely to pay a premium for protection. Tsai *et al.* (2011) found that purchases from websites by experimental subjects were strongly influenced by graphics indicating the extent of privacy protection and the extent to which privacy protection deviates from the subjects' privacy requirements. Likewise (and similar to the results of Beresford *et al.* 2012), they found that subjects simply bought goods from the least expensive websites in a treatment in which privacy information was not prominently displayed.

50.0 The privacy paradox also diminishes where subjects are able to compare privacy promises in connection with the sale of goods side-by-side. In those situations, they are more willing to pay a premium for increased privacy. Egelman *et al.* (2013). Also, Egelman *et al.* (2009) found that subjects were more likely to take privacy concerns into account when privacy information could be viewed *before* visiting a website, rather than *after* arriving at a website—timing also influences whether individuals act to protect their privacy.

51.0 Finally, the privacy paradox also tends to disappear in studies that measure people's economic value of protecting their PII. Economic value is measured either in terms of willingness to pay ("WTP") or willingness to accept ("WTA"). WTP is the maximum amount of money a person would pay voluntarily to avoid releasing (or to maintain secrecy over) their PII.

52.0 Importantly, WTP is not what an individual *actually* pays to protect PII from release; it is the maximum amount (including consumer surplus) that person would pay if "push came to shove.". In other words, when a good is purchased, the actual payment for that good (the price per unit) is usually a fraction of WTP. WTP to protect personal information, therefore, measures the value of the information, because a person would be indifferent between the alternatives of: (a) paying the money and protecting the information and (b) not paying the money and releasing the information.

53.0 By contrast, the related concept of WTA refers to the minimum amount of money a person would demand for the loss of security over their PII. Conceptually, the values of WTP and WTA should be about the same, but when measured empirically, WTA often turns out to be

the larger of the two. In the privacy context, for example, Acquisti *et al.* (2013) found WTA estimates about five to six times larger than WTP estimates, depending on context and phrasing of questions. Possible reasons for this outcome include loss aversion (people may see greater harm in losing a small amount of security over their privacy details than they see benefit in a small increase privacy security) and the fact that WTP is budget constrained (subjects have limited funds with which to pay), while WTA is not (subjects are not limited in the amount they can ask for).

54.0 In any event, this discrepancy is another potential hurdle to valuing privacy promises and PII accurately. In addition, this consideration suggests that the more conservative measure, WTP, may be more appropriate in this matter.

55.0 Because PII protection is usually bundled together with the sale of goods and services in commerce (as here), the value of protecting the PII is not directly revealed in these transactions—there is no separate line-item for privacy protection in typical transactions such as the App sales here.[31] As a result, there are no direct measures for the value a consumer is willing to pay to protect their PII. Furthermore, if there was an unauthorized disclosure of PII after a transaction that included PII protection, there is no direct measure of the WTA compensation for the disclosure.

56.0 As a result, empirical valuation studies generally rely on data from stated preference field studies using CV methodology or laboratory experiments. Although some controversy remains, CV methods have been widely used in valuing goods that are not traded in explicit markets (e.g. non-market goods such as fewer health risks, cleaner air, preservation of the last members of an endangered species, and protection of PII). The values for WTP are derived from posing hypothetical questions in a survey.

57.0 The first study to measure the value protection of PII (Hann *et al.* (2002)) applied conjoint analysis to data obtained in a laboratory experiment using undergraduate students. The experiment was concerned with aspects of protecting such information when contacting an

[31] It may be indirectly revealed, but economists have not fully worked out how to do so reliably.

internet website. A key finding was that protecting personal data against errors, restricting personal data from secondary use and improper access were worth between $45.61 and $57.01.

58.0 A recent laboratory experiment conducted by Benndorf and Normann (2014) examined experimental subjects' (university students) willingness to sell (i.e., WTA) varying bundles of personal information. Five such bundles were studied: (1) preferences (including information about hobbies, political views, shopping behavior, income, age, gender, and occupation); (2) contact data (including name, address, e-mail address, and telephone number); and (3) the subjects' Facebook Timeline and About pages. Values for WTA were established by a reverse second price auction, which is used extensively in laboratory experiments and has been shown to have desirable value revealing properties.

59.0 Mean values of willingness to sell the various attribute bundles were as follows: (1) preferences (€8.32), (2) contact data (€14.88), (3) preferences and contact data (€18.90), (4) Facebook About page (€17.67), and (5) Facebook Timeline page (€19.49). In a related study, Bauer *et al.* (2012) obtained estimates of WTP to buy back PII from Facebook. As might be expected (as discussed above, WTP is often smaller than WTA), the WTP was indeed considerably smaller than the corresponding WTA estimated by Benndorf and Normann (2014).

60.0 In a more recent study, Savage and Waldman (2015) conducted a choice experiment using CV methods to estimate WTP to grant privacy permissions when purchasing smartphone apps. Savage and Waldman report that in their survey of 1,726 smartphone users the representative consumer was willing to make one-time payments per App purchased of: (1) $2.28 to conceal their browser history, (2) $4.05 to conceal their contacts list, (3) $1.19 to conceal their location, (4) $1.75 to conceal their phone's identification number, and (5) $3.58 to conceal their texts. Split sample estimates also were obtained to show the extent of variation in these values by age, income, education, and gender.

61.0 In another study closely related to Savage and Wildman, Butler and Glasgow (2014) estimated the value of different types of personal information in the context of purchasing hypothetical streaming video services. Survey respondents were presented with eleven alternative scenarios that were subject to experimental control. Scenarios consisted of different:

(1) levels of privacy policy, (2) numbers of videos available, (3) content availability, (4) commercial advertising policy, and (5) prices per month. The following WTP values were found: (1) $3.90 per month for promise that the vendor will not share video usage information with third-parties, and (2) $5.99 per month for a promise that the vendor will not share both video usage information and PII with third parties. These values represent substantial fractions of the highest price that respondents were shown ($12.99).

62.0 The most recent studies by Savage and Waldman (2015) and Butler and Glasgow (2014) demonstrate that the value of PII (similar to the PII at issue in this case) can be quantified to a reasonable degree of economic certainty by using CV surveys and the econometric techniques. The study executed for this Report follows the methodologies used in these two studies.

**iii. The Survey**

63.0 To quantify the PII value wrongly disclosed in this case, I designed a CV study very similar in structure to the ones used recently by Savage and Waldman (2015) and by Butler and Glasgow (2014). Specifically, I administered a survey to a large sample of qualified respondents to estimate their WTP to grant privacy permissions of various types that are at issue in this case when purchasing a smartphone App.

64.0 I recognize that here, the Buyers' PII has already been disclosed and the harm done. One might assume that I should therefore try to measure WTA (a payment in compensation for the disclosure), but this would be wrong in this particular case for two reasons.

65.0 First, the economic harm in this case is that the Buyers did not get the benefit of the bargain. The Buyers received the App and the processing services, but not the privacy protection. So really, the issue is determining the value of the privacy protection that the Buyers purchased, but did not receive—this is a WTP question.

66.0 Second, as noted above, WTA measures can overstate damages in some circumstances. Again, this is because WTA (how much would you ask for?) is not bounded by the budget of the injured party as WTP is (how much would you pay for?). Also, WTA results may be too speculative because Buyers are not as familiar with novel situations such as payment

in compensation for a breach of promised privacy—Buyers lack a baseline for this kind of transaction. So, to be conservative and realistic, the survey was designed to obtain answers for WTP, not the usually much higher WTA.

67.0 Counsel requested that I quantify the value of each of the following sets of privacy breaches at issue in this case: (1) privacy with no disclosure of PII; (2) disclosure of name and email; (3) disclosure of state, city, and zip code; (4) disclosure of email, name, city, state, and zip; (5) disclosure of email, name, street, city, and zip; (6) disclosure of email, name, street, city, zip, and phone number.

68.0 Alternative 1, privacy with no disclosure of PII, was what the Plaintiff was to receive by contract. This alternative serves as a control or base case. Based on the discovery in this matter, Alternative 2 through Alternative 6 represent sets of PII that were wrongly disclosed.

69.0 To quantify a respondent's WTP, each respondent was presented with a hypothetical purchase of an App at a particular price bundled with one of the alternative packages of privacy protection. Each respondent was only presented with one alternative and one price. This referendum-style of question is considered very reliable, because respondents are not offered successive prices or package. The prices ranged from $1 to $5 for each alternative.

70.0 Exhibit #5 contains the survey instrument. The survey begins with two qualifying or screening questions. First, respondents were asked whether they own a smart phone. If they did, the survey continued; if not, then the survey ended and they were not included. Second, respondents were asked whether they had ever purchased an App for their smart phone. Only those who had purchased an App were allowed to continue in the survey. The screening questions made sure that respondents would understand the survey question and answer reliably. As noted above, each qualifying respondent was presented with a hypothetical purchase of an App at a particular price bundled with a set of privacy protections. The respondent would either be willing to purchase or not.

71.0 The hypothetical purchase was presented in the following way: "We want to know how you feel about new APPs for smart phones. We have just a few questions to ask. Suppose that the APP Store has a new APP available that you are very interested in purchasing.

Suppose you are a returning customer to the APP Store, so you know that the Store already has your name, email address, billing address, mobile number, and credit card number." This question was designed to mimic the facts of this case whereby Buyers would have already disclosed to Defendants the same PII by the time they were about to purchase an App.

72.0 Then the respondent would be presented with an alternative set of privacy protections and a price. For example, following the description of the App, the respondent would be presented with for example Alternative #2 for $2, as follows: "The App Store has a strict policy of not sharing any of your information with the developer or seller of the App you are interested in except for your name and email. Would you be willing to pay $2 for this App that you want?" The yes or no answer would then be recorded.

73.0 Finally, the respondent was asked for certain demographic and economic information, including year of birth, income, ethnicity, and education.

**C. Survey Results**

74.0 The survey was conducted by Opinion Access Corp. between February 5, 2016 and March 2, 2016. Initially, over 200 web based surveys were completed on February 13, 2016 as a soft pre-test. These initial results confirmed that respondents understood the survey and that the pricing parameters were appropriate in that all price points received positive and negative responses. At this juncture the full survey moved ahead over the web and with landline and mobile phone subsets added. The results included 5,019 completed web surveys, 46 mobile phone surveys, and 39 landline respondents.

75.0 The survey design relies primarily on the web-based survey responses. The mobile phone and landline subsets were designed strictly as controls to assess the reliability of the web-based survey. The limited results from the mobile phone and land line surveys confirm the reliability of the web based survey by demonstrating that: (a) respondents understood the questions; (b) all combinations of privacy alternatives and prices had market relevance; and (c) the demographic and ethnic compositions of the web sample compared to the landline or the mobile phone sample were similar (no statistically significant differences).

76.0 The survey sample size of 5,019 completions provides highly reliable and robust results. This large sample size results in over 800 respondents for each of the six alternative bundles of PII at issue in this case. To generate reliable responses for each of the six alternatives at the 99% level of confidence with a margin of error of +/- 5% would require a sample size of 525 respondents.[32] The actual sample size of respondents achieved exceeds this threshold.

77.0 Table 3 summarizes the survey results. These summary results show that Defendants' privacy-protection obligations represented a valuable portion of what the Buyers paid for. On average, 75% of respondents would have paid for the App with the maximum privacy protection compared to only 64%-to-70% who would purchase the App with lower levels of privacy protection. Furthermore, with only two exceptions at the $5 price point, respondents preferred the highest level of privacy protections.

**Table 3. Summary of Survey Results**

| **Alternative #1 – Privacy with No Disclosure** | **Yes** | **No** | **Total** | **% Yes** | **% No** |
|---|---|---|---|---|---|
| **$1.00** | 148 | 19 | 167 | 89% | 11% |
| **$2.00** | 135 | 31 | 166 | 81% | 19% |
| **$3.00** | 127 | 41 | 168 | 76% | 24% |
| **$4.00** | 118 | 56 | 174 | 68% | 32% |
| **$5.00** | 103 | 62 | 165 | 62% | 38% |
| | ==== | ==== | ==== | | |
| **Total** | 631 | 209 | 840 | **75%** | 25% |
| | | | | | |
| **Alternative #2 – Share Name and Email** | | | | **% Yes** | **% No** |
| **$1.00** | 123 | 44 | 167 | 74% | 26% |
| **$2.00** | 135 | 31 | 166 | 81% | 19% |
| **$3.00** | 110 | 56 | 166 | 66% | 34% |
| **$4.00** | 107 | 63 | 170 | 63% | 37% |
| **$5.00** | 112 | 55 | 167 | 67% | 33% |
| | ==== | ==== | ==== | | |
| | 587 | 249 | 836 | **70%** | 30% |

[32] Sample size is calculated as a function of: (a) margin of error, (b) confidence level, and (c) sample variation. See Thompson (1992) for further details.

| **Alternative #3 – Share State, City, and Zip** | | | | **% Yes** | **% No** |
|---|---|---|---|---|---|
| **$1.00** | 137 | 31 | 168 | 82% | 18% |
| **$2.00** | 126 | 41 | 167 | 75% | 25% |
| **$3.00** | 118 | 47 | 165 | 72% | 28% |
| **$4.00** | 103 | 64 | 167 | 62% | 38% |
| **$5.00** | 103 | 64 | 167 | 62% | 38% |
| | ==== | ==== | ==== | | |
| | 587 | 247 | 834 | **70%** | 30% |
| | | | | | |
| | | | | | |
| **Alternative #4 – Share Email, Name, City, State, and Zip** | | | | **% Yes** | **% No** |
| **$1.00** | 138 | 28 | 166 | 83% | 17% |
| **$2.00** | 116 | 50 | 166 | 70% | 30% |
| **$3.00** | 109 | 56 | 165 | 66% | 34% |
| **$4.00** | 115 | 55 | 170 | 68% | 32% |
| **$5.00** | 107 | 62 | 169 | 63% | 37% |
| | ==== | ==== | ==== | | |
| | 585 | 251 | 836 | **70%** | 30% |
| | | | | | |
| | | | | | |
| **Alternative #5 – Share Email, Name, Street, City, and Zip** | | | | **% Yes** | **% No** |
| **$1.00** | 127 | 38 | 165 | 77% | 23% |
| **$2.00** | 127 | 41 | 168 | 76% | 24% |
| **$3.00** | 107 | 59 | 166 | 64% | 36% |
| **$4.00** | 106 | 61 | 167 | 63% | 37% |
| **$5.00** | 110 | 60 | 170 | 65% | 35% |
| | ==== | ==== | ==== | | |
| | 577 | 259 | 836 | **69%** | 31% |
| | | | | | |
| **Alternative #6 – Share Email, Name, Street, City, Zip, and Phone #** | | | | **% Yes** | **% No** |
| **$1.00** | 120 | 46 | 166 | 72% | 28% |
| **$2.00** | 113 | 52 | 165 | 68% | 32% |
| **$3.00** | 111 | 60 | 171 | 65% | 35% |
| **$4.00** | 100 | 68 | 168 | 60% | 40% |
| **$5.00** | 89 | 78 | 167 | 53% | 47% |
| | ==== | ==== | ==== | | |
| | 533 | 304 | 837 | **64%** | 36% |

78.0 It is no surprise that Buyers value the security of their PII, for the reasons the literature has already pointed out, as discussed above. In this case, too, it appears that Google has

acknowledged consumers' reluctance to share PII. Both Google and consumers[33] recognize that sharing PII can cause security problems for users.[34]

79.0

Therefore, the survey results whereby respondents prefer the App with greater privacy protection and are willing to pay more for them appears consistent with the evidence in the case.

[33] *See* Elbouchikhi Dep. Tr. 209:18 – 23

[34] GOOG-00005451 – 58 GOOG-00002087

[35] You Dep. Tr. 138:38

[36] *Id.* at 207:19 – 24.

[37] Affaki Dep. Tr. 92:12 – 13, 94 You Dep. Tr. 132:7 – 14 .

[38] GOOG-00005154 GOOG-00005156 GOOG-00005169

**D. Econometric Analysis of the Survey Results**

80.0 The survey results were summarized in Table 3. In this section, I used econometric analysis to quantify the values for Buyers' WTP for an App along with various levels of privacy protection based on the survey results. Survey respondents were presented with a hypothetical App purchase along with a complement of privacy protection at a specific price. As in the real marketplace, the respondent could either make the purchase or not. Since this was a "take it or leave it" proposition, the Buyer did not have to come up with a price – instead the price was provided ($1, $2, $3, $4, or $5). This methodology is consistent with the referendum style of questions found to be reliable in CV surveys.

81.0 However, to estimate the Buyers' WTP the survey data was analyzed using a standard statistical technique called regression analysis. Regression analysis is a statistical technique use to analyze the relationship among variables, in this case among the bundles of PII and price. Essentially, a regression analysis quantifies the relationship between the variable of interest and a set of explanatory variables. In this case, the analysis focuses on whether a Buyer would purchase an App with a particular bundle of privacy protections at a price that varies from $1 to $5.

82.0 To determine these figures, I used a standard logit regression model. The technique is a type of regression model widely used to analyze binary dependent variables (that is variables that are either 1 or 0—the yes or no data I collected in the survey).[39] Here, the economic model explains the probability that a Buyer will purchase the App and its complement of privacy protection at a particular price. Some Buyers are willing to make the purchase (scored as 1); others are not (scored as 0).

83.0 Table 4 summarizes the regression results for the model using the logit approach. The complete regression output is available in Exhibit #6. The logit model fits the data well in that all of the regression coefficients have their expected signs and each is statistically significant at the 99% level of confidence.

[39] Wooldridge, Jeffery (2013), Introductory Econometrics, Southwestern: Mason, Ohio, pages 583 – 589.

**Table 4. Logit Analysis of the App Purchase Choices**

| Variable | Coefficient | Std. Error | z-Statistic | Prob. |
|---|---|---|---|---|
| **No Privacy Disclosure** | 1.798939 | 0.107952 | 16.66424 | 0 |
| **Disclosure of Name and Email** | 1.547145 | 0.104293 | 14.83459 | 0 |
| **Disclosure of State, City, and Zip** | 1.553835 | 0.104374 | 14.88719 | 0 |
| **Disclosure of Email, Name, City, State, and Zip** | 1.537149 | 0.104254 | 14.74434 | 0 |
| **Disclosure of Email, Name, Street, City, and Zip** | 1.490771 | 0.103626 | 14.38609 | 0 |
| **Disclosure of Email, Name, Street, City, Zip, and Phone** | 1.244809 | 0.100716 | 12.35962 | 0 |
| **App Price $1-$5** | -0.222837 | 0.022299 | -9.992973 | 0 |

84.0 As expected, the coefficient on price is negative, and as the price increases from $1 to $5 for the purchase, the probability of purchase decreases. The coefficients for the alternative packages are all positive as expected, and they vary depending upon the type of privacy protection provided. The standard errors for the coefficient estimates are very low, so that each is statistically significant with a zero probability of equaling zero. This means that the regression results are reliable for analytical purposes.

85.0 To determine the WTP (in this case, to pay less) for each of the alternatives, two steps are required. First, I take the difference between the coefficient for full privacy protection, and each of the other alternatives with less privacy protection. Second, I divide the result of step 1 by the coefficient on Price. Table 5 shows the calculations.

86.0 Thus, Buyers are willing to pay $2.49 to avoid the significant disclosure of their PII associated with Alt 6 compared to $1.10 to avoid the less amount of PII disclosed under Alt3. The other alternatives vary in general relationship to the amount of PII disclosed.

**Table 5. Calculation of WTP**

| Alternative | Difference from Alt1 | WTP More Privacy |
|---|---|---|
| **Disclosure of Name and Email (Alt 2)** | -$0.25 | $1.13 |
| **Disclosure of State, City, and Zip (Alt 3)** | -$0.25 | $1.10 |
| **Disclosure of Email, Name, City, State, and Zip (Alt 4)** | -$0.26 | $1.17 |
| **Disclosure of Email, Name, Street, City, and Zip (Alt 5)** | -$0.31 | $1.38 |
| **Disclosure of Email, Name, Street, City, Zip, and Phone (Alt 6)** | -$0.55 | $2.49 |

87.0 The results presented in Table 5 are consistent with the results in other recent studies that quantified the WTP for privacy protection by Savage and Waldman (2013) and by

Butler and Glasgow (2014) discussed above.[40] Although the databases and specific choices offered to consumers were different, the results are reasonably comparable.

### E. Calculating the Benefit-of-the-Bargain Damages Using the Formulae

88.0 As noted above, the benefit-of-the-bargain damages can be estimated for any Buyer, for any price paid for an App, and for any of the sets of PII wrongly disclosed using the three formulae provided above. Table 4 provides the estimates for the WTP for the contracted-for privacy (PP) and for the various bundles of privacy that were wrongfully disclosed ("D1" through "D5"). These data are used along with the price paid for the App to quantify the damages under the benefit-of-the-bargain theory.

89.0 Following the formulae, the values for the % privacy delivered are calculated using the coefficient estimates from Table 4. For each alternative disclosure bundle ("D1" through "D5"), the % privacy delivered is the ratio of the coefficient for the disclosure type divided by the coefficient for the contracted-for privacy.

90.0 For example, the % privacy delivered when there was disclosure of the name and email is calculated from the values in Table 4 as: 1.547145 / 1.798939 = 0.86. The discount for this bundle of disclosure is then is 1 - 0.86 = 0.14 or 14%.

91.0 In this case for example, the Plaintiff purchased the App for $1.77. So, the damage associated with the disclosure of the name and email address is $0.25, calculated as 14% of the Price paid of $1.77. Table 6 repeats these calculations for the other disclosure bundles.

**Table 6. Calculations for the Benefit-of-the-Bargain Damages**

| Privacy Disclosure | % Privacy Delivered | Discount | Price | Damage |
|---|---|---|---|---|
| **Disclosure of Name and Email** | 86% | 14% | $1.77 | **$0.25** |
| **Disclosure of State, City, and Zip** | 86% | 14% | $1.77 | **$0.24** |
| **Disclosure of Email, Name, City, State, and Zip** | 85% | 15% | $1.77 | **$0.26** |
| **Disclosure of Email, Name, Street, City, and Zip** | 83% | 17% | $1.77 | **$0.30** |
| **Disclosure of Email, Name, Street, City, Zip, and Phone** | 69% | 31% | $1.77 | **$0.55** |

92.0 On a $1.77 App purchase, Damages vary from $0.24 to $0.55 depending upon the type of disclosure. All of this is by way of illustrating how the formulae work. The formulae are

[40] Similar statistical techniques were used as well to generate the WTP shown in Table 5.

applicable to all Buyers regardless of the actual price they paid for their App, and demonstrate that benefit-of-the-bargain damages can indeed be calculated on a class-wide basis.

**F. Testing the Regression Equation**

93.0 I conducted a number of tests on the database which all produced similar results. This indicates that the results presented above in Tables 4 – 6 are robust, meaning that changes in the regression techniques do not result in significant changes in the conclusions.

94.0 For example, I re-estimated the model using a probit regression instead of a logit regression as described above. Either technique is appropriate to use with limited dependent variables of interest in this case. The difference between the two estimators is the statistical assumption concerning the dispersion of the data or the disturbance in the system. The disturbance term in a logit model is assumed to follow a logistic function while in the probit model the disturbance term is assumed to be normally distributed.

95.0 Table 7 provides a summary of the probit estimates for the model. The full regression results are found in Exhibit #6. Again, all of the coefficient estimates have the expected signs and each is highly significant at the 99% confidence level. This means that the coefficient estimates can be reliably used for analytical work.

**Table 7. Probit Analysis of the App Purchase Choices**

| Variable | Coefficient | Std. Error | z-Statistic | Prob. |
|---|---|---|---|---|
| | | | | |
| **ALT1** | 1.100233 | 0.063745 | 17.26 | 0 |
| **ALT2** | 0.944886 | 0.061874 | 15.27119 | 0 |
| **ALT3** | 0.951403 | 0.062159 | 15.30596 | 0 |
| **ALT4** | 0.940248 | 0.062036 | 15.15661 | 0 |
| **ALT5** | 0.911567 | 0.061719 | 14.76973 | 0 |
| **ALT6** | 0.762276 | 0.060659 | 12.56658 | 0 |
| **PRICE** | -0.135155 | 0.013382 | -10.0996 | 0 |

96.0 Of course, the absolute magnitudes of the coefficients estimated by probit are different from those estimated by logit. However, the ultimate results for the damage estimates are very similar. Following the same procedure used to estimate the benefit-of-the-bargain damages using logit, with the probit coefficient estimates, produces the results shown in Table 8.

As the results are quite similar to the ones from Table 6, this means that the methodology and the results are reliable and robust.

**Table 8. Calculations for the Benefit-of-the-Bargain Damages using Probit**

| Privacy Disclosure | % Privacy Delivered | Discount | Price | Damage |
|---|---|---|---|---|
| **Disclosure of Name and Email** | 86% | 14% | $1.77 | **$0.25** |
| **Disclosure of State, City, and Zip** | 86% | 14% | $1.77 | **$0.24** |
| **Disclosure of Email, Name, City, State, and Zip** | 85% | 15% | $1.77 | **$0.26** |
| **Disclosure of Email, Name, Street, City, and Zip** | 83% | 17% | $1.77 | **$0.30** |
| **Disclosure of Email, Name, Street, City, Zip, and Phone** | 69% | 31% | $1.77 | **$0.54** |

97.0 As shown in Table 8, the damage estimates range from $0.24 to $0.54. These are all comparable to the damages estimated using logit in Table 6, which ranged from $0.24 to $0.55. Thus, the choice of regression technique does not affect the damage estimate.

98.0 It is therefore my opinion that the methodology and equations identified above can be used to calculate the benefit-of-the-bargain damages for any Buyer who had his or her PII improperly disclosed by Defendants, and that such damages may be calculated in the same matter on a class-wide basis among Buyers similarly situated.

## VI. Quantifying Diminished Value of Buyers' PII

99.0 In addition to Defendants depriving Buyers of the benefit of their bargain, Plaintiff also asserts that Defendants' PII disclosures harmed her and other App Buyers by usurping their ability to sell their own PII. As a result, App buyers lost the sales value of that information.[41] This section of my report quantifies damages attributable to this loss of the sales value of the PII at issue.

100.0 There is no doubt that an active PII-purchasing market exists. Consumer data, and the information marketplace supporting the online advertising industry in the United States, is estimated at about $26 billion per year.[42] The Federal Trade Commission has stated that consumer data has inherent monetary value within the information marketplace: "Most

[41] *See* Dkt. 118 at 8 – 9.

[42] See Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, WSJ.com (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html

consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[43] Additionally, major companies including Acxiom, Tableau Software, and Red Hat, focus on the acquisition and marketing of PII. Other major technology companies are also major players in this field, and include companies such as HP, Oracle, Microsoft, and Accenture.

101.0 In addition, the robust market for PII is not restricted to business-to-business sales. Increasingly, individuals are able to sell their PII themselves: Various companies offer individuals the opportunity to sell their PII and PII-related information.[44]

102.0 Over the last few years, a number of new companies began offering to manage personal information and sell it under controlled circumstances paying individuals for that purpose. The three most prominent companies in this space are Datacoup,[45] Handshake,[46] and Meeco.[47] While each of them takes a different approach to managing and monetizing PII on behalf of their users, they all demonstrate that consumers are beginning to recognize the value of their PII and are taking steps to exploit that value for their own benefit.

103.0 Datacoup provides compensation to its users depending upon how much information the user is willing to share and the value and sensitivity of that information. NPR reported that users can earn about $8 per month for allowing access to their Twitter or Foursquare profiles.[48]

104.0 Handshake is an app and a website that allows users to negotiate a price for their personal data directly with the companies that want to buy it. Handshake was designed for people who recognize that their personal data has value. Handshake notes that "Rewards come in many forms and money is only one option. Total rewards can vary hugely depending on how

---

[43] Pamela Jones Harbour, Remarks Before FTC Exploring Privacy Roundtable, Federal Trade Commission, 2 (Dec. 7, 2009), available at http://www.ftc.gov/sites/default/files/documents/public_statements/remarksftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[44] *See* Joshua Brustein, Start-Ups Seek to Help Users Put a Price on Their Personal Data, N.Y. Times (Feb. 12, 2012), http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-ontheir-personal-data.html.

[45] https://datacoup.com/

[46] http://handshake.uk.com

[47] https://meeco.me/

[48] http://www.npr.org/2014/09/09/346981606/privacy-or-profit-these-firms-want-to-help-you-sell-your-data

unique your Handshake is, how much data you put in your profile (how visible you are to those brands, basically) and how many brands you want to engage with."[49]

105.0 Meeco claims to help clients securely manage and control their digital relationships. By using Meeco's private cloud to store information and share users' brand preferences, clients would expect discounts on their purchases.

106.0 The existence of these companies illustrates not only that PII has a market value and can be actively traded on an exchange, but that it is also feasible for individuals to do so.

107.0 [redacted]

108.0 [redacted]

109.0 [redacted]

[49] http://handshake.uk.com/hs/faq.html.

[50] GOOG-00001490 [redacted]

[51] *See* Elbouchikhi Dep. Tr. 40:17 – 20 [redacted]

[52] *See* GOOG-00002260 – 67.

[53] *See, e.g.*, GOOG-00003976 [redacted]

[54] *See, e.g.*, GOOG-00003976 – 83; Affaki Dep. Tr. 82:17 – 24 [redacted]; *id.* at 130:12 – 19 [redacted]

110.0 [redacted]

111.0 Because the Defendants furnished App Vendors with this Buyer PII information in violation of its privacy promises with Buyers, the Buyers were denied the opportunity of exploiting their PII's value themselves, thereby causing damage.

112.0 To calculate the diminution of Buyer PII resulting from Defendants providing it to third parties—thereby depriving Buyers from profiting from their PII—I surveyed published reports in order to determine prices. Published reports indicate that data marketers sell personal information on average for $0.083 per person when bundled in groups of 1,000 individuals.[58] However, the value of the PII depends upon its specificity and sensitivity. General information about a consumer such as age, gender, or location may be worth only $0.0005 per person, or $0.50 per 1,000 people. However, the value increases significantly if the person is shopping for a car, a financial product, or a vacation. For $0.26 per person, buyers can purchase lists of email addresses for people with specific healthcare conditions.[59]

113.0 In this case, the PII that was disclosed may have included at least one or more of the following: Email, Name, Street, City, Zip, and Phone Number. This set of PII falls into the

---

[55] *See, e.g.*, GOOG-00003976 – 3983; Affaki Dep. 92:8 – 23 [redacted]

[56] Elbouchikhi Dep. Tr. 26:4 – 27:1 [redacted]

[57] Powers Dep. Tr. 37:8 – 16 [redacted]

[58] Billy Ehrenberg, *How much is your personal data worth*, The Guardian (Apr. 22, 2014), http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth.

[59] Emily Steel, et al., *How much is your personal data worth?*, Financial Times (June 12, 2013), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz42czqK6Th.

general category of PII sold in the marketplace that I found. Published reports indicate such information is marketed at an average price of $0.083 per person.

114.0 A number of companies offer to provide sales leads containing similar bundles of PII. Their pricing for various combinations of PII provides a basis for estimating the value of the PII disclose, and Defendants' disclosures deprived Buyers of the ability to exchange that valuable information with vendors on their own terms. In other words, instead of being provided for free by Google, the PII could have been sold by Class Members for roughly the same amounts depending upon the bundle of PII offered for sale.

115.0 Table 9 provides a summary of the values at which various combinations of PII can be readily purchased in the marketplace in batches of 10,000. Prices vary from $0.080 for names and addresses up to $0.170 for names, addresses, emails, and phone numbers. While there is some value added by the vendors in providing large volumes of PII by location, this value added is offset in this case for two reasons.

**Table 9. Diminished Value of PII**

| Type/Category of PII | Value |
|---|---|
| **General/Average** | $0.083 |
| **Name and address** | $0.080 |
| **Name, address, and email** | $0.100 |
| **Name, address, and phone number** | $0.100 |
| **Name, address, and email campaign** | $0.110 |
| **Name, address, email, and phone number** | $0.170 |

Sources: InfoUSA, LeadsPlease.com; The Guardian, Alesco Data, Redidata, and Accurate Leads, Axciom, NAICS Association, LLC, and Nationwide Marketing Services

116.0 First, the PII in this case was tied to specific App purchases, making the value of the PII disclosed to third parties even more meaningful for marketing purposes. [redacted].[60]

[60] Elbouchikhi Dep. Tr. 39:8 – 10 [redacted].

117.0 Second, the PII in this case—tied to a valid payment method and based on a recent and actual purchase—indicates that the PII is fresh (as opposed to being a cold lead). Again, this helps explain why the PII in this case was valuable and sought after by App Vendors.[61]

118.0 Therefore, it is my opinion that the unauthorized disclosure of Buyers' PII in this case diminished the value of the PII disclosed by $0.08 to as much as $0.17 per Buyer. Further, diminution-of-value damages may be calculated in the same matter on a class-wide basis among Buyers similarly situated.

**Discovery Developments May Warrant an Update**

119.0 Should additional information become available that would materially alter my analysis, I would update this report accordingly.

120.0 However, at this time based on the information available to me, my report is complete.

Date: April 7, 2016

Henry Fishkind, Ph.D

[61] *See* GOOG-00002260 – 67.

**CERTIFICATE OF SERVICE**

I hereby certify that on April 7, 2016, I served the above and foregoing by transmitting it to the persons shown below by electronic mail.

Susan D. Fahringer
sfahringer@perkinscoie.com
Charles C. Sipos
csipos@perkinsoie.com
Breena M. Roos
broos@perkinscoie.com
Mica Simpson
msimpson@perkinscoie.com
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101

s/ J. Dominick Larry